## AMENDMENTS TO THE SPECIFICATION AND ABSTRACT

***In the specification, page 1, after the title, please insert the following heading:***

BACKGROUND OF THE INVENTION

***In the specification, page 1, line 5, please amend the sub-heading as follows:***

1. ~~Technical~~ Field of Invention

***In the specification, page 1, line 10, please amend the sub-heading as follows:***

2. ~~Background~~ Description of the Related Art

***In the specification, page 7, line 3, please amend the sub-heading as follows:***

~~Disclosure~~ Brief Summary of the Invention

***In the specification, page 7, lines 19-23, please amend the paragraph as follows:***

In order to solve such a problem, it is effective if a generated prime allows ~~to identify which~~ identification of the server that has generated the prime. Since an RSA public key is computed by multiplication of two different primes, even if another key issuing server generates the same primes by chance, it is possible to eliminate these primes.

***In the specification, page 7, 24-28, please amend the paragraph as follows:***

Given this factor, the present invention aims at offering a prime calculating apparatus for calculating primes whose generation source can be identified, a prime verification apparatus for performing the identification~~-~~, a key issuing system, a prime calculation method, a prime verification method, and a computer program.

***In the specification, page 10, lines 3-8, please amend the paragraph as follows:***

In addition, the prime generation unit may (i) generate a combination of the issue identifier and a variable c that is one of 0 and a positive integer, (ii) calculate a prime candidate = 2 × prime g × f(the combination) + 1,- and (iii) test primality of the calculated prime candidate, and outputs the calculated prime candidate as the prime gp when the primality of the calculated prime candidate is determined.

***In the specification, page 17, lines 27-28 to page 18, lines 1-20, please amend the paragraph as follows:***

Here, the prime calculating apparatus may further (i) store a different verification value from the verification value, (ii) newly obtain a prime N' by calculating a prime candidate N', according to N' = 2 × multiplication value R × prime q + the different verification value, (iii) calculate a number n, according to n = prime N × prime N', using the prime N and the newly obtained prime N' and generates a random number e, and (iv) calculate d satisfying e × d = 1 mod L, where L is a least common multiple of the prime N - 1 and the prime N' - 1, and a combination of the calculated number n and the generated random number e is the public key while the calculated d is the private key. In this case, the prime-verification-apparatus information storage unit stores the different verification value, and the obtaining unit obtains the combination of the number n and the random number e as the public key. The verifying unit includes: a subtraction subunit operable to obtain a multiplication value by multiplying the verification value and the different verification value and to obtain a public key subtraction value by subtracting the multiplication value from the obtained number n; a judgment subunit operable to judge whether the obtained prime subtraction value is divisible by the management information; and a control subunit operable to permit output of the public key when the judgment is affirmative, and prohibit the output of the public key when the judgment is negative.

***In the specification, page 23, lines 20-28 to page 24, lines 1-28 to page 25, lines 1-28 to page 26, lines 1-28 to page 27, lines 1-27, please amend the paragraph as follows:***

~~*Explanation of References*~~

~~1 key issuing system~~

~~100, 101, 102 key issuing server~~

~~110 identifier repository~~

~~111 private key repository~~

~~112 public key repository~~

~~113 certificate repository~~

~~114 control unit~~

~~115 identifier generation unit~~

~~116 prime generation unit~~

~~117 key judgment unit~~

~~118 key generation unit~~

~~119 information acquisition unit~~

~~120 reception unit~~

~~121 transmission unit~~

~~130 server identifier storage area~~

~~131 terminal information storage area~~

~~132 iteration control unit~~

~~133 prime information generation unit~~

~~135 iteration counter~~

~~136 output counter~~

~~140 information control unit~~

~~141 random number generation unit~~

~~142 prime candidate generation unit~~

~~143 1st primality testing unit~~

~~144 2nd primality testing unit~~

~~200 certificate issuing server~~

~~210 private key repository~~

~~211 issue public key repository~~

~~212 issue identifier information repository~~

~~213 public key certificate repository~~

~~214 issue public key determination unit~~

~~215 public key certificate generation unit~~

~~216 certificate acquisition unit~~

~~217 reception unit~~

~~218 transmission unit~~

~~220 server information storage area~~

~~221 determination information storage area~~

~~300, 301, 302, 303, 304, 305, 306 terminal~~

~~310 private key repository~~

~~311 public key certificate repository~~

~~312 control unit~~

~~313 accepting unit~~

~~314 radio unit~~

~~315 baseband signal process unit~~

~~316 speaker~~

~~317 microphone~~

~~318 display unit~~

~~319 antenna~~

~~320 terminal identifier storage area~~

~~400 terminal~~

~~2 key issuing system~~

~~1100, 1101, 1102 key issuing server~~

~~1110 identifier repository~~

~~1111 private key repository~~

~~1112 public key repository~~

~~1113 certificate repository~~

~~1114 control unit~~

~~1115 identifier generation unit~~

~~1116 prime generation unit~~

~~1117 key judgment unit~~

~~1118 key generation unit~~

~~1119 information acquisition unit~~

~~1120 reception unit~~

~~1121 transmission unit~~

~~1122 certificate generation unit~~

~~1123 certificate private key repository~~

~~1124 issued key information repository~~

~~1130 server identifier storage area~~

~~1131 terminal information storage area~~

~~1200 key issuing audit server~~

~~1210 determination information repository~~

~~1211 issued key information repository~~

~~1212 control unit~~

~~1213 issue public key determination unit~~

~~1214 accepting unit~~

~~1215 audit-result output unit~~

~~1216 reception unit~~

~~1217 transmission unit~~

~~1220 server information storage area~~

~~1250 monitor~~

~~1300, 1301, 1302, 1303, 1304, 1305, 1306 terminal~~

~~1400 terminal~~

~~2100 prime generating apparatus~~

~~2101 accepting unit~~

~~2102 accepted information storage unit~~

~~2103 prime seed generation unit~~

~~2104 random number generation unit~~

~~2105 prime candidate generation unit~~

~~2106 1st primality testing unit~~

~~2107 2nd primality testing unit~~

~~2200 prime generating apparatus~~

~~2201 accepting unit~~

~~2202 accepted information storage unit~~

~~2203 random number generation unit~~

~~2204 prime candidate generation unit~~

~~2205 1st primality testing unit~~

~~2206 2nd primality testing unit~~

~~2300 prime generating apparatus~~

~~2301 accepting unit~~

~~2302 accepted information storage unit~~

~~2303 identifier prime generation unit~~

~~2304 random number generation unit~~

~~2305 prime candidate generation unit~~

~~2306 1st primality testing unit~~

~~2307 2nd primality testing unit~~

~~2400 prime generating apparatus~~

~~2401 accepting unit~~

~~2402 accepted information storage unit~~

~~2403 random number generation unit~~

~~2404 prime candidate generation unit~~

~~2405 1st primality testing unit~~

~~2406 2nd primality testing unit~~

~~2500 prime generating apparatus~~

~~2501 accepting unit~~

~~2502 accepted information storage unit~~

~~2503 random number generation unit~~

~~2504 prime candidate generation unit~~

~~2505 1st primality testing unit~~

~~2506 2nd primality testing unit~~

***In the specification, page 28, line 46, please amend the heading as follows:***

~~Best Mode for Carrying Out~~ Detailed Description of the Invention

***In the specification, page 94, lines 13-16, please amend the paragraph as follows:***

Receiving the order to start prime generation from the identifier generation unit 115, ~~-~~the iteration control unit 132C sets both the iteration counter 135C and output counter 136C to "1".

***In the specification, page 177, line 11, please amend the sub-heading as follows:***

~~Industrial Applicability~~

***In the Abstract, please amend as follows:***

~~The present invention offers a~~ A prime calculating apparatus ~~for~~ calculating a prime and determining ~~which can be determined~~ whether ~~it~~ the prime has been duly generated. The prime calculating apparatus (i) generates a random number, (ii) calculates a multiplication value R by multiplying a management identifier by the random number, and (iii) calculates a prime candidate N, according to N = 2 × (multiplication value R + w) × prime q + 1, with respect to w satisfying an equation of 2 × w × prime q + 1 = verification value (mod management information). Then, the prime calculating apparatus judges whether the calculated prime candidate N is a prime, and outputs the calculated prime candidate N as a prime when determining that it is a prime.